

Albuquerque
CYBER TASK FORCE

Standard Memorandum of Understanding

Between

THE FEDERAL BUREAU OF INVESTIGATION

and

ALBUQUERQUE POLICE DEPARTMENT

I. PARTIES

This Memorandum of Understanding (MOU) is entered into by and between the Federal Bureau of Investigation (FBI) Albuquerque Division and the Albuquerque Police Department (APD).

II. AUTHORITIES

The FBI is authorized to coordinate intelligence, investigative, and operational responses to cyber threats, attacks, and intrusions pursuant to various statutory and executive authorities, including 28 U.S.C. § 533; 42 U.S.C. § 3771; 28 C.F.R. § 0.85; Executive Order 12333, *as amended*; the Attorney General's Guidelines for Domestic FBI Operations; Annex II to NSPD-46/HSPD-15; NSPD-54/HSPD-23 and 18 U.S.C. §1030, 50 U.S.C. § 1801 *et seq.*

III. PURPOSE

- A. The Comprehensive National Cybersecurity Initiative (CNCI) was formally established in 2008 pursuant to NSPD-54/HSPD-23. The CNCI recognizes the need for a whole-of-government approach to protecting the nation from cybersecurity threats. To further this mission, NSPD-54/HSPD-23 also established the National Cyber Investigative Joint Task Force (NCIJTF), which serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. In accordance with this presidential directive, the NCIJTF operates under the authority of the Attorney General. The Director of the FBI is the designated official responsible for the operation of the NCIJTF. The NCIJTF enhances collaboration and integrates operations among the represented U.S. Intelligence Community and federal law enforcement partners.

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Cyber Task Force
Standard MOU
August 2018

*This document is the property of the FBI.
Neither it nor its contents may be released without authorization by FBI Headquarters.*

- B. While national-level coordination is important to securing the nation, teamwork at the local level is also essential. The FBI has established a nationwide network of field office Cyber Task Forces (CTFs) to focus on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners with many of the federal agencies that participate in the NCJTF at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level.
- C. This MOU delineates the responsibilities and commitments of the FBI and the Participating Agency in the Albuquerque CTF.
- D. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agency, the United States, or the officers, employees, agents, or other associated personnel thereof.

IV. MISSION

- A. In support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each CTF synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.
- B. Each CTF leverages the authorities and capabilities of the participating agencies to accomplish the mission.
- C. Recognizing the important role of the private sector in combating the cyber threats facing our nation, each CTF will coordinate with private sector entities to the extent permissible by law and as warranted by operational needs, as set forth by separate agreements between the FBI and these private sector entities.

V. SUPERVISION AND CONTROL

- A. Overall management of the CTF shall be the responsibility of the Assistant Director in Charge (ADIC) or Special Agent in Charge (SAC) of the Albuquerque Division of the FBI and/or his or her designee.
- B. All guidance on investigative matters handled by the CTF will be issued by the Attorney General or the FBI. The FBI will make available to the Participating Agency applicable guidelines and policies, including the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) and the FBI's Domestic Investigations and Operations Guide (DIOG).
- C. The ADIC or SAC shall designate one Supervisory Special Agent to supervise day-to-day operational and investigative matters pertaining to the CTF (CTF Supervisor).

VI. STAFFING COMMITMENT AND RESPONSIBILITIES

- A. In addition to FBI employees, each CTF may consist of the following types of individuals: Task Force Officers, Task Force Members, and Task Force Participants. For purposes of this MOU, when referring to these individuals collectively, they will be referred to as "CTF personnel." In brief, the DIOG defines these terms as follows:
1. Task Force Officer (TFO): The individual is a certified law enforcement officer, authorized to carry a firearm, has been deputized under Title 18 of the U.S. Code, been issued Federal law enforcement credentials, is assigned to the supervision of the CTF, has an active security clearance recognized by the FBI, and is authorized to have access to FBI facilities.
 2. Task Force Member (TFM): The individual is an employee of a governmental agency, is assigned to the supervision of the CTF, has an active security clearance recognized by the FBI, and is authorized to have access to FBI facilities.
 3. Task Force Participants (TFPs): The individual participates on the CTF and does not otherwise qualify as a TFO or TFM. A TFP is sometimes referred to as a "Task Force Liaison."
- B. In light of the significant cost and effort in on-boarding new CTF personnel, and need for continuity to successfully combat cyber threats, each Participating Agency agrees to provide its personnel to the CTF for a period of at least two (2) years. This MOU imposes no maximum limit as to the time that any individual may remain on the CTF.
- C. During periods of heightened threats and emergencies, the CTFs may need to operate 24 hours per day for an extended period of time. To function properly, the CTF depends upon the unique contributions of each Participating Agency. During these periods, all CTF personnel are expected to be available to support CTF activities unless released to the Participating Agency.
- D. Due to the operational needs of the CTF, assignment to special details or duties outside of the CTF to full-time CTF personnel by the Participating Agency must be coordinated with the CTF Supervisor.
- E. On a case-by-case basis, CTF Supervisors may authorize CTF personnel to assist other non-CTF priority FBI matters as necessary and as legally permissible.
- F. Although CTF personnel will report to his or her Participating Agency for non-investigative administrative matters, leave requests will be coordinated with the CTF Supervisor to ensure staffing availability.
- G. Non-FBI CTF personnel remain subject to the rules, regulations, laws, and policies applicable to employees of the participant's respective agency and will also adhere to the FBI's ethical standards and the Supplemental Standards of Ethical Conduct for employees of the Department of Justice (DOJ). Where there is a conflict between the standards or requirements of the Participating Agency

and the FBI, the standard or requirement that provides the greatest organizational protection or benefit will apply, unless the FBI and the Participating Agency jointly resolve the conflict otherwise.

- H. CTF personnel must adhere to the same rules and regulations as FBI employees with regard to security policies, conduct and activities while in FBI space, handling FBI property, while operating FBI vehicles, and while conducting CTF business.
- I. Continued assignment to the CTF will be based on performance and at the discretion of each CTF member's Participating Agency. The FBI ADIC or SAC will also retain discretion to remove any member from the CTF.
- J. CTF personnel are subject to removal from the CTF by the FBI for violation of any provision of this MOU, the FBI's ethical standards, the Supplemental Standards of Ethical Conduct for employees of the DOJ, or other applicable agreements, rules, and regulations.

VII. DEPUTATION/SECURITY CLEARANCE/DEADLY FORCE POLICY

- A. Non-federal personnel who will serve on the CTF as a TFO will be federally deputized under Title 18 of the U.S. Code while detailed to the CTF. The FBI will secure the required authorization for their deputation. This will ensure that they are able to assist fully in investigations in compliance with applicable federal statutes.
- B. CTF personnel may be required to handle sensitive and classified information, have access to classified systems, and/or have access to secure office space. Therefore, participants must be eligible to obtain and maintain an appropriate security clearance, up to and including Top Secret, and access to Sensitive Compartmented Information (SCI). CTF personnel being granted access to SCI must successfully complete an annual Security Financial Disclosure Form and counterintelligence (CI) focused polygraph examination. The FBI will recognize counterintelligence polygraph examinations conducted by outside federal agencies that meet the FBI's PSPP requirement, if the polygraphers administering the examination are accredited by the National Center for Credibility Assessment and the candidate successfully completed the examination within the past five (5) years. The FBI will make the final determination whether a polygraph examination meets the PSPP requirements. All CTF personnel will execute non-disclosure agreements deemed necessary by the FBI for the protection of classified and sensitive information, including but not limited to an SF-312, Classified Nondisclosure Agreement. Supervisors in the Participating Agency responsible for CTF personnel may only be provided with classified information if they have the appropriate security clearance to receive the classified information and the requisite "need to know."
- C. CTF TFOs will follow the Participating Agency's policy concerning use of deadly force.

VIII. COORDINATION

- A. Intelligence, law enforcement, and operational actions will be coordinated and cooperatively carried out within the CTF. The Participating Agency will not act unilaterally on any matter affecting the CTF. The parties agree that matters designated to be handled by the CTF shall not knowingly be subject to non-CTF or non-FBI intelligence, law enforcement, or operational efforts by the Participating Agency.
- B. On occasion, after coordination with and approval by the CTF Supervisor, a CTF TFO or TFM may handle an investigation solely under the Participating Agency's authorities. In such a case, the investigation will be supervised by the Participating Agency and conducted under the authority of the Participating Agency.
- C. CTF criminal investigative procedures will conform to the requirements for federal prosecution. It is expected that the appropriate U.S. Attorney, in consultation with the FBI and affected CTF partners, will determine on a case-by-case basis whether the prosecution of cases will be at the federal or state level, based upon which would better advance the interests of justice.
- D. All media releases will be mutually agreed upon, jointly handled by the Participating Agencies, and conform to DOJ guidelines. No press release involving a CTF matter will be issued without prior FBI approval.

IX. INFORMATION SHARING/REPORTS AND RECORDS

- A. Except as described in paragraph VIII.B above, all investigative and intelligence reporting will be prepared and disseminated in compliance with FBI policy. Subject to any legal or policy restrictions, copies of documents created for a CTF matter based upon information obtained from participation on the CTF by any CTF personnel will be considered to be a federal document under the control of the FBI and shall be maintained in accordance with FBI records management policy and applicable law. All CTF materials and investigative records, including any Memoranda of Understanding, originate with, belong to, and will be maintained by the FBI. All CTF investigative reports will be prepared by CTF personnel solely on FBI forms.
- B. All information learned during the course of a CTF investigation will be subject to the FBI's information sharing policies and may not be disclosed outside of the CTF (or removed, if in tangible form, from FBI space) without the approval of the CTF Supervisor. As FBI records, they may be disclosed only with FBI permission from the CTF Supervisor and only in conformance with the provisions of federal laws and regulations, including the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act of 1974, 5 U.S.C. § 552a, as well as applicable civil and criminal discovery privileges. CTF personnel may not disclose any FBI or CTF-related information outside of the CTF, including any disclosure to CTF personnel's own Participating Agency, without the prior approval of

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Cyber Task Force
Standard MOU
August 2018

*This document is the property of the FBI.
Neither it nor its contents may be released without authorization by FBI Headquarters.*

the FBI CTF Supervisor. Participating Agency heads will be routinely briefed on CTF matters by the ADIC, SAC, or CTF Supervisor, as appropriate, through established CTF briefings.

- C. CTF personnel are strictly prohibited from disclosing any classified information to individuals who do not possess the appropriate security clearance and the need to know. Each Participating Agency agrees to have its CTF personnel sign an FD-868, or a similar form approved by the FBI. This action obligates the participant, who is accepting a position of special trust in being granted access to classified and otherwise sensitive information as part of the CTF, to be bound by prepublication review to protect against the unauthorized disclosure of such information.
- D. The FBI and Participating Agency acknowledge that the information involved in this MOU may identify individuals whose information may be protected by the Privacy Act of 1974 and "United States persons" whose information may be protected by Executive Order 12333, as amended (or any successor thereto) and all such information shall be handled lawfully pursuant to the provisions thereof, to the extent applicable.
- E. CTF personnel may be required to handle and process Protected Critical Infrastructure Information (PCII), as defined by law and regulated by the U.S. Department of Homeland Security (DHS). All CTF personnel will use and disclose DHS PCII in accordance with applicable law and regulation.
- F. The FBI and Participating Agency will immediately report to each other each instance in which data received from each other is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches).
- G. The FBI and Participating Agency agree to abide by the DOJ Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment (January 25, 2010) to the extent that any CTF-related information is covered by that policy. At a minimum, the FBI and Participating Agency shall notify each other of any erroneous information concerning United States citizens or legal permanent resident aliens that is disclosed pursuant to this MOU and take reasonable steps to correct such error.

X. SALARY/OVERTIME COMPENSATION/FUNDING

- A. The FBI and Participating Agency agree to assume all personnel costs for their CTF personnel, including salaries, overtime payments and fringe benefits.
- B. Subject to funding availability and legislative authorization, the FBI may reimburse to Participating Agency the cost of overtime worked by non-federal CTF members assigned full-time to CTF, provided overtime expenses were incurred as a result of CTF-related duties. A separate Cost Reimbursement Agreement (CRA) must be executed between the FBI and Participating Agency, consistent with regulations and policy. Otherwise, overtime shall be compensated in accordance

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Cyber Task Force
Standard MOU
August 2018

*This document is the property of the FBI.
Neither it nor its contents may be released without authorization by FBI Headquarters.*

with applicable Participating Agency overtime provisions and shall be subject to the prior approval of appropriate personnel.

- C. Subject to funding availability and legislative authorization, the FBI may provide a lease vehicle, fuel purchase card, and smart phone to non-federal full-time CTF personnel for use in carrying out CTF-related duties. Receiving personnel will be required to execute acceptable use agreements before being issued these items.
- D. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds. Even where one of the parties to this MOU has agreed (or later does agree) to assume a particular financial responsibility, such party's express written approval must be obtained before incurring any expense expected to be assumed by the other party. All obligations of and expenditures by the parties to this MOU will be subject to each party's respective budgetary and fiscal processes and availability of funds pursuant to all applicable laws, regulations, and policies. The parties to this MOU acknowledge that there is no intimation, promise, or guarantee that funds will be available in future years.

XI. TRAVEL

All CTF-related travel of non-FBI personnel requires the approval of the CTF Supervisor and Participating Agency authorization prior to travel. To avoid delay in operational travel, the Participating Agency will provide general travel authority to all of its participating employees for the duration of the employee's membership in the CTF. For domestic travel, CTF personnel will be responsible for appropriate notifications within his or her Participating Agency, as well as standard FBI travel approvals and notification. The CTF will obtain FBI Headquarters authorization and country clearances for CTF personnel required to travel outside the United States. The FBI will pay costs for travel in accordance with the Federal Travel Regulations of all CTF personnel to conduct investigations outside the field office territory.

XII. LIABILITY

- A. General. The Participating Agency acknowledges that financial and civil liability, if any and in accordance with applicable law, for the acts and omissions of each employee detailed to the CTF remains vested with his or her employing agency. However, DOJ may, in its discretion, determine on a case-by-case basis that an individual should be afforded legal representation, legal defense, or indemnification of a civil judgment, pursuant to federal law and DOJ policy and regulations.

1. Common Law Tort Claims

- a. Congress has provided that the exclusive remedy for the negligent or wrongful act or omission of an employee of the U.S. Government, acting within the scope of his or her employment, shall be an action against the United States under the Federal Tort Claims Act (FTCA), 28 U.S.C. § 1346(b), and §§ 2671 - 2680.

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Cyber Task Force
Standard MOU
August 2018

*This document is the property of the FBI.
Neither it nor its contents may be released without authorization by FBI Headquarters.*

- b. Notwithstanding any other provision contained in this MOU, for the limited purpose of defending civil claims arising out of CTF activity, any employee detailed from a Participating Agency who is acting within the course and scope of his or her official duties and assignments pursuant to this MOU may be considered an “employee” of the U.S. Government, as defined at 28 U.S.C. § 2671. See 5 U.S.C. § 3374(c)(2).
- c. Under the Federal Employee Liability Reform and Tort Compensation Act of 1998 (commonly known as the Westfall Act), 28 U.S.C. § 2679(b)(1), if an employee of the United States is named as a defendant in a civil action, the Attorney General or his or her designee may certify that the defendant acted within the scope of his or her employment at the time of the incident giving rise to the suit. 28 U.S.C. § 2679(d)(2). The United States can then be substituted for the employee as the sole defendant with respect to any tort claims alleged in the action. 28 U.S.C. § 2679(d)(2). If the United States is substituted as defendant, then “any other civil action or proceeding for money damages arising out of or relating to the same subject matter against the employee or the employee’s estate is precluded without regard to when the act or omission occurred.” 28 U.S.C. § 2679(b)(1).
- d. If the Attorney General declines to certify that an employee was acting within the scope of employment, “the employee may at any time before trial petition the court to find and certify that the employee was acting within the scope of his office or employment.” 28 U.S.C. § 2679(d)(3).
- e. Liability for any negligent or willful acts of CTF personnel undertaken outside the terms of this MOU will be the sole responsibility of the respective employee and agency involved.

2. Constitutional Claims

- a. Liability for violations of federal constitutional law may rest with the individual federal agent or officer pursuant to Bivens v. Six Unknown Names Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) or pursuant to 42 U.S.C. § 1983 for state officers.
- b. Federal, state, local, and tribal officers enjoy qualified immunity from suit for constitutional torts, “insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.” Harlow v. Fitzgerald, 457 U.S. 800 (1982).
- c. If any Participating Agency’s CTF personnel is named as a defendant in his or her individual capacity in a civil action alleging constitutional damages as a result of conduct taken within the scope of CTF-related duties, the individual may request representation by DOJ. 28 C.F.R. §§ 50.15, 50.16.

- d. An employee may be provided representation “when the actions for which representation is requested reasonably appear to have been performed within the scope of the employee’s employment, and the Attorney General, or his or her designee, determines that providing representation would otherwise be in the interest of the United States.” 28 C.F.R. § 50.15(a).
- e. Any CTF personnel’s written request for representation should be directed to the Attorney General and provided to the Chief Division Counsel (CDC) of the FBI division coordinating the CTF. The CDC will forward the representation request to the FBI’s Office of the General Counsel (OGC), together with a letterhead memorandum concerning the factual basis of the lawsuit. FBI’s OGC will then forward the request to the Civil Division of DOJ, together with an agency recommendation concerning scope of employment and DOJ representation. 28 C.F.R. § 50.15(a)(3).
- f. If any CTF personnel is found to be liable for a constitutional tort, he or she may request indemnification from DOJ to satisfy an adverse judgment rendered against the employee in his or her individual capacity. 28 C.F.R. § 50.15(c)(4). The criteria for payment are substantially similar to those used to determine whether a federal employee is entitled to DOJ representation under 28 C.F.R. § 50.15(a).
- g. Determinations concerning legal representation and indemnification by the United States are discretionary and are made by DOJ on a case-by-case basis. The FBI cannot guarantee that the United States will provide legal representation, legal defense, or indemnification to any federal or state employee detailed to the CTF, and nothing in this MOU shall be deemed to create any legal right on the part of any CTF personnel.

B. Express Reservations

- 1. Nothing in this Article shall be deemed to create an employment relationship between the FBI or the United States and any Participating Agency CTF member other than for exclusive purposes outlined in the Liability section herein.
- 2. The Participating Agency does not waive any available defenses and/or limitations on liability. No Participating Agency shall be considered to be an agent of any other Participating Agency.

XIII. DURATION

- A. The term of this MOU is for the duration of the CTF's operation, contingent upon approval of necessary funding, but may be terminated at any time upon written mutual consent of the Participating Agency involved.

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Cyber Task Force
Standard MOU
August 2018

*This document is the property of the FBI.
Neither it nor its contents may be released without authorization by FBI Headquarters.*

- B. Any Participating Agency may withdraw from the CTF at any time by written notification to the ADIC or SAC or the National Cyber Task Force Unit at FBI Headquarters at least 30 days prior to withdrawal.
- C. Upon termination of this MOU, all equipment provided to the CTF will be returned to the supplying Participating Agency(ies). In addition, when a Participating Agency withdraws from the MOU, the Participating Agency will return equipment to the supplying Participating Agency(ies). Similarly, any remaining Participating Agency will return to a withdrawing Participating Agency any unexpended equipment supplied by the withdrawing Participating Agency.

XIV. MODIFICATIONS

This agreement in no manner affects any existing agreements with the FBI or any other agency. This agreement may be amended only by mutual written consent of the parties. The modifications shall have no force or effect unless such modifications are reduced to writing and signed by an authorized representative of the FBI and the Participating Agency.

XV. SIGNATORIES

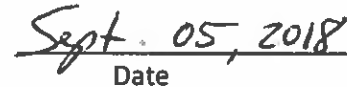
Name:

Date

Title:

Organization:


Name: James C. Langenberg


Date

Title: Special Agent in Charge

Organization: Federal Bureau of Investigation

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Cyber Task Force
Standard MOU
August 2018

*This document is the property of the FBI.
Neither it nor its contents may be released without authorization by FBI Headquarters.*